ORIGINAL

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	

COMMENTS OF AT&T

Amanda E. Potter
Gary L. Phillips
David Lawson
AT&T SERVICES, INC.
1120 20th Street, NW
Washington, DC 20036

Kevin G. Rupy
Kathleen Scott
WILEY REIN LLP
1776 K Street, NW
Washington, DC 20006

July 24, 2019

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	

COMMENTS OF AT&T

AT&T Services, Inc.[1] hereby submits these comments in response to the *Third Further Notice of Proposed Rulemaking* ("*FNPRM*") adopted by the Federal Communications Commission ("Commission") proposing "to allow voice service providers to block calls based on caller ID authentication in certain instances," the development of a critical calls list, as well as seeking comment on whether to require implementation of the SHAKEN/STIR protocols, among other proposals.[2]

INTRODUCTION AND SUMMARY

AT&T applauds this important step toward establishing appropriate safe harbors for provider-initiated call blocking. Indeed, AT&T has made no secret of its desire to more aggressively target illegal and unwanted robocalls on its network. AT&T is working every day to protect its customers from the onslaught of robocalls through its innovative call blocking and

---

[1] AT&T Services, Inc. is filing these comments on behalf of its wireless and wireline operating affiliates (collectively, "AT&T").

[2] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, FCC 19-51, ¶ 48 (rel. June 7, 2019) ("*Dec. Ruling and FNPRM*").

labeling programs. Since late 2016, when AT&T led the industry by introducing AT&T Call Protect, the first provider-branded call blocking service, AT&T has blocked or labeled nearly **600 million** suspected fraud calls and more than **1.4 billion** suspected spam calls through the AT&T Call Protect suite of products.[3] In addition, apart from these tools, AT&T's global fraud team identifies and blocks traffic it believes to be illegal, and has blocked more than **5 billion** such calls on AT&T's network.[4] Most recently, AT&T announced that it would add automatic fraud blocking and suspected spam-call alerts to millions of customers on an opt-out basis and at no charge—another industry first.[5] The expansion of the Call Protect service was made possible by the Commission's recent Declaratory Ruling ("*Opt-Out Call Blocking Declaratory Ruling*"),[6] which represents a major milestone in the fight against illegal and unwanted robocalls.

The *FNPRM*, which proposes to establish an appropriate safe harbor to encourage more aggressive blocking by voice service providers, would mark an even more significant milestone, and AT&T urges the Commission to act decisively and without delay. Consumer, regulator, and legislator calls for more effective solutions to the robocall problem seemingly multiply in number and volume by the day, but they are dwarfed by the growing avalanche of illegal and unwanted robocalls plaguing consumers. While call blocking is not, and never will be, the sole answer to the problem of illegal and unwanted robocalls, the Commission should promptly acknowledge the integral role that effective provider-initiated call blocking can and should play

---

[3] Letter to Commissioner Starks from Joan Marsh, Executive Vice President, Regulatory & State External Affairs, to Commissioner Starks, FCC, Regulatory & State External Affairs (filed July 10, 2019), https://docs.fcc.gov/public/attachments/DOC-358443A2.pdf (last visited July 24, 2019).

[4] *Id.*

[5] Press Release, AT&T, AT&T Call Protect Expands Service (July 9, 2019) https://about.att.com/story/2019/att_call_protect.html (last visited July 10, 2019).

[6] *Dec. Ruling and FNPRM.*

in turning the tide against the entities generating such calls. Accordingly, consistent with the authority conferred under Sections 201 and 202 of the Communications Act, as amended (the "Act"), AT&T urges the Commission to adopt a broad safe harbor that would empower providers to target and remove illegal robocalls from their networks, while also providing appropriate incentives for providers to adopt the SHAKEN/STIR standards.

While AT&T supports efforts to encourage broader deployment of SHAKEN/STIR, SHAKEN/STIR verification of a particular call should not be the touchstone for protection under a safe harbor.[7] Instead, the Commission should look to AT&T's proposed safe harbor, which would afford protection to voice providers for call blocking programs that are based on reasonable, good-faith efforts to target and eliminate illegal traffic. Further, AT&T supports conditioning application of the safe harbor to voice providers that have implemented SHAKEN/STIR. Such a safe harbor, building on the Commission's proposal, would encourage deployment not only of SHAKEN/STIR, but also of other analytical tools to help determine whether a call is illegal, and thus would directly serve the public interest.

The Commission also should take care to avoid undermining the efficacy of providers' existing call blocking programs or creating unnecessary loopholes that fraudsters can (and will) exploit. In AT&T's view, an overly proscriptive approach would only thwart, rather than advance, the Commission's and industry's efforts to tackle the robocall problem. By the same token, the Commission should make clear that any safe harbor it adopts would cover a provider in the event it inadvertently blocks a legitimate call. Simply put, a safe harbor limited to

---

[7] AT&T uses the terms "authentication" and "verification" herein in a manner consistent with the standards. "Authentication" is the process by which an *originating* voice provider inserts a digital signature to signal that the calling number is deemed to be legitimate and allowed to be used by the calling party. In contrast, "verification" is the process used by a *terminating* voice provider to validate the digital signature. The two processes are related yet distinct.

insulating providers from liability for blocking *illegal* calls would do nothing to promote more aggressive action by industry, as the Commission already has confirmed that no risk of liability exists for such calls.

Finally, AT&T welcomes the Commission's interest in additional measures that would enhance the ability of industry to prevent illegal and unwanted calls from ever reaching consumers, including by targeting blocking activity to specific voice providers that have demonstrated a willingness to facilitate the origination of illegal traffic. AT&T looks forward to continuing to work with the Commission and other industry stakeholders to pursue an appropriate framework for such blocking activity, as well as other innovative approaches to combat illegal and unwanted robocalls.[8]

ARGUMENT

I. THE COMMISSION SHOULD ADOPT A SAFE HARBOR THAT ENCOURAGES MORE AGGRESSIVE PROVIDER BLOCKING OF ILLEGAL ROBOCALLS AND INCENTS PROVIDERS TO ADOPT THE SHAKEN/STIR STANDARDS

AT&T shares the Commission's strong commitment to the deployment of the SHAKEN/STIR standards, given the important role the standards will play in addressing illegal robocalls. Indeed, AT&T helped to develop the SHAKEN/STIR protocols and is one of the major service providers currently deploying the technology in its network. AT&T co-authored

[8] While these initial comments will focus on the proposal to establish a call blocking safe harbor, AT&T agrees that SHAKEN/STIR must be widely deployed to be effective. With respect to the *FNPRM*'s request for comment on whether to require deployment, AT&T has not opposed such a mandate, but AT&T remains cautiously optimistic that such a mandate will prove unnecessary. Nonetheless, AT&T will not hesitate to join those calling for an implementation requirement if it becomes evident that the goal of achieving industry-wide implementation compels the adoption of rules. And with respect to the important issue of protecting the outbound calls of emergency responders, AT&T is working closely with its industry partners to address the complex questions raised in the *FNPRM*, as reflected in the comments filed by the industry associations.

the standards themselves.[9] Additionally, AT&T's Martin Dolly chairs the working group developing the technical standards for SHAKEN/STIR, and AT&T holds the chairmanship of the industry board overseeing the SHAKEN/STIR effort.[10] Already, 100 percent of AT&T's consumer VoIP and consumer post-paid VoLTE calls originating on AT&T's network are authenticated, and AT&T and Comcast are exchanging authenticated calls between our two separate networks.[11] AT&T currently is testing with two other service providers and is ready to test with others once they are ready. By the end of this year, AT&T expects that nearly all calls originating on AT&T's IP networks that are eligible for full attestation, including FirstNet, will be authenticated.

While AT&T views SHAKEN/STIR as an important tool, AT&T nevertheless cautions the Commission that basing any safe harbor solely on the SHAKEN/STIR framework likely would encourage provider-initiated blocking in only very narrow circumstances and, in any event, has the potential for serious unintended consequences. AT&T therefore urges the Commission to establish a call blocking safe harbor consistent with AT&T's prior proposals, modified as appropriate to incent the broader deployment of SHAKEN/STIR.

A. The SHAKEN/STIR Standards Should Play an Important—But Not Determinative—Role in Voice Provider Call Blocking Programs.

Notwithstanding its important role in combating illegal robocalls, SHAKEN/STIR is not

---

[9] *See* Martin Dolly, An Introduction and Overview of the STIR/SHAKEN Framework, SIP FORUM (Dec. 11, 2018)(*"STIR/SHAKEN Framework"*), https://www.sipforum.org/download/an-introduction-and-overview-of-the-stir-shaken-framework/ (last visited July 24, 2019).

[10] *See* STI-GA Leadership, https://www.atis.org/sti-ga/leadership/ (last visited July 24, 2019).

[11] *AT&T, Comcast Announce Anti-Robocalling Fraud Milestone Believed to be Nation's First*, AT&T (Mar. 20, 2019), https://about.att.com/story/2019/anti_robocall.html (last visited July 24, 2019).

a suitable tool for determining whether a call is illegal, much less unwanted. Accordingly, AT&T agrees with the concerns raised by several industry experts at the Commission's July 11 SHAKEN/STIR Robocall Summit ("July 11 Summit") regarding the proposal to establish a narrow safe harbor based solely on SHAKEN/STIR verification information.[12]

Numerous experts, including at the July 11 Summit, have explained that the presence or absence of SHAKEN/STIR verification *on its own* is neither necessary nor sufficient to indicate that a call should be blocked today. As AT&T's Martin Dolly, a co-author of both the SHAKEN and STIR standards, has noted, the standards validate the caller ID information associated with a call and identify the attesting provider.[13] While this certainly is useful information for providers to have when making blocking decisions, it is important to recognize its limitations. This sentiment was repeated time and again at the Commission's July 11 Summit.[14] One panelist there noted that even in the case of a fully attested call, "it could still be the devil himself calling from a verified number."[15] Another panelist noted that determinations regarding whether a call

---

[12] *Dec. Ruling and FNPRM* ¶¶ 50, 51 (making the assumption that it "will provide a strong basis for call blocking.").

[13] *See* Martin Dolly, *An Introduction and Overview of the STIR / SHAKEN Framework*, AT&T (Dec. 4, 2018) (*"AT&T Presentation"*), https://www.sipforum.org/download/an-introduction-and-overview-of-the-stir-shaken framework/?wpdmdl=3530&refresh=5d2e1ad1a6bdc1563302609) (last visited July 16, 2019). Chris Wendt of Comcast, who co-authored both standards, stated that SHAKEN/STIR alone would not determine "whether the call is illegitimate or legitimate, or what the intent of the call is, or what the content of the call is." Chris Wendt, Director of Technical Research & Development for IP Communications, Comcast, and Co-author of SHAKEN and STIR standards, Statement at the July 11 Summit, at 00:08:07 – 00:08:26 (July 11, 2019) (*"Wendt Statement"*).

[14] *See SHAKEN/STIR Robocall Summit*, FCC (July 11, 2019), https://www.fcc.gov/SHAKENSTIRSummit (last visited July 18, 2019) (*"July 11 Summit"*).

[15] *See* Scott Hambuchen, Chief Information Officer, First Orion, Statement at the July 11 Summit, at 1:43:21 – 1:43:40 (July 11, 2019) (*"Hambuchen Statement"*).

is unwanted or illegal were a "hard thing in general," and a more suitable approach is to leave such determinations to "analytics and other tools."[16] One panelist went as far as to say that, in the context of a blocking decision, "deploying a STIR/SHAKEN solution without any analytic solution behind it . . . can be dangerous."[17]

As the Commission has stated, "SHAKEN/STIR does not authenticate the content of the call," but instead only authenticates the associated caller ID.[18] The Alliance for Telecommunications Industry Solutions ("ATIS")—the industry-led organization helping to successfully establish this important caller ID authentication framework—has explained that the SHAKEN standard "was never intended to be a complete solution for the robocalling problem," and is instead "an important tool in a multi-layered approach."[19] ATIS describes the SHAKEN/STIR standards as a framework designed to achieve two discrete purposes: "the authentication and assertion of a telephone identity by an originating service provider," and "the verification of the telephone identity by a terminating service provider."[20] ATIS has further emphasized that "information on the 'intent' [of a call] was never part of SHAKEN,"[21] and that the standard "verifies that the entity originating a call is entitled to use the phone number

---

[16] *Wendt Statement* at 00:08:07 – 00:08:26.

[17] *Hambuchen Statement* at 2:03:15 – 2:03:32.

[18] Report on Robocalls: A Report of the Consumer and Governmental Affairs Bureau, Consumer and Governmental Affairs, ¶ 21 (Feb. 14, 2019) ("*FCC Robocall Report*"), https://docs.fcc.gov/public/attachments/DOC-356196A1.pdf (last visited July 24, 2019).

[19] ATIS SHAKEN FAQ, at 7, https://www.atis.org/01_strat_init/dlt/docs/shaken-faq.pdf (last visited July 11, 2019) (*"SHAKEN FAQ"*).

[20] ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN), Alliance for Telecommunications Industry Solutions, Approved January, at 3, ATIS-1000074.

[21] *SHAKEN FAQ* at 7.

displayed – nothing more!"[22] It also has stated that, while SHAKEN is focused on "verifying the source of the call," other separate, yet complementary, mechanisms (such as network intelligence, know-your-customer initiatives, and other call analytics) focus on the "intent of the call."[23]

In short, more is needed than SHAKEN/STIR information to enable a provider to determine whether a call should be blocked.[24] AT&T expects that technical network-related errors will be responsible for most, if not all, instances in which SHAKEN/STIR verification fails—particularly in the early days of implementation ahead of the existence of a complete administrative framework—not because the calling party spoofed the originating telephone number or attempted to subvert the SHAKEN/STIR process. And such "failures" are to be expected as implementation proliferates and providers continue to learn from the individualized provider-to-provider implementations. Thus, for these and potentially other reasons, a call that fails SHAKEN/STIR verification may be perfectly legitimate and, in fact, wanted by the receiving party.

Similarly, a call that has been authenticated and verified under SHAKEN/STIR may be an illegal (or unwanted) call, as the example above from the July 11 Summit demonstrates. The mere fact that the call received full attestation and verification cannot on their own demonstrate that the call is legal and wanted, and should not be determinative of whether a provider should or should not block the call. Rather, providers should consider SHAKEN/STIR attestation (full,

---

[22] Jim McEachern, *SHAKEN & Know Your Customer*, ATIS, at 3 (Oct. 2018), https://access.atis.org/apps/group_public/download.php/43134/IPNNI-2018-00129R001.pptx (last visited July 11, 2019) (emphasis in original) (*"ATIS Presentation"*).

[23] *Id.* at 13.

[24] *See Dec. Ruling and FNPRM* ¶ 53.

partial, or gateway) information,[25] together with other data points, to make a reasonable determination about blocking.

This view also is consistent with the findings of the North American Numbering Council Call Authentication Trust Anchor Working Group ("NANC CATA WG") referenced in the *FNPRM*.[26] The NANC CATA WG acknowledged that a safe harbor would provide a "strong incentive for communications service provider adoption of SHAKEN" and, further, noted that such a safe harbor would be particularly useful "where analytics are overlaid on the framework."[27] In other words, any safe harbor construct established by the Commission should account for both SHAKEN/STIR verification *and other factors*, such as the data aggregated and used as part of AT&T's network-level call blocking program and, separately, the AT&T Call Protect product suite. Analytics are crucial to any safe harbor framework because, unlike the SHAKEN/STIR standards, analytics are specifically designed for making judgments regarding the likely content of a call and thus whether the call should be blocked.

B. A Call Blocking Safe Harbor That Relies on SHAKEN/STIR Also Could Undermine Efforts To Fight Illegal Robocalls.

Given the limitations of SHAKEN/STIR, AT&T cautions the Commission to avoid establishing a safe harbor—or any other legal or regulatory mechanism—that could result in unintended negative consequences, including but not limited to, chilling provider innovation and

---

[25] It is important to note here as well that *full* SHAKEN/STIR information—including whether a call receives full, partial, or gateway attestation—is more valuable than partial SHAKEN/STIR information that simply indicates whether a call has failed verification.

[26] *Dec. Ruling & FNPRM* ¶ 49 n.101.

[27] NANC Call Authentication Trust Anchor Working Group, Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR, at 14 (May 3, 2018), http://nanc-chair.org/docs/mtg_docs/May_18_Call_Authentication_Trust_Anchor_NANC_Final_Report.pdf (last visited July 8, 2019) (*"NANC CATA WG Report"*).

experimentation in the robocall mitigation space and/or rendering the SHAKEN/STIR standards ineffective by establishing a system that fraudsters could easily circumvent.

First, the Commission should avoid tying providers' hands in ways that would impede their ability to adapt in reaction to the evolving tactics of bad actors. For example, should the Commission describe or explain its safe harbor in negative terms—*i.e.*, by stating what providers may *not* do—voice providers could feel foreclosed from continuing to engage in call blocking activities that they have found effective, but which arguably fall outside the technical scope of the safe harbor. The result in such circumstances would be a net decrease in the number of suspected illegal calls blocked as compared to today, and thus would be contrary to the Commission's goals.

Second, and relatedly, the Commission should avoid creating technological loopholes that would prompt bad actors to develop practices and procedures to evade the SHAKEN/STIR framework. At least at the outset, the Commission should expect that provider-initiated blocking programs largely will hue to the parameters of any adopted safe harbor. To the extent the Commission's safe harbor does not afford providers sufficient flexibility to evolve, any safe harbor quickly could lose effectiveness and would not produce the desired results, particularly given the highly adaptive and innovative nature of the fraudsters.[28]

According to one expert at the Commission's July 11 Summit, industry is facing "intelligent adversaries" that are "actively trying to fight back against companies" blocking their calls, and these same adversaries "will be reacting to STIR/SHAKEN, and we are already

[28] Similarly, because a safe harbor limited to calls that fail SHAKEN/STIR is unlikely to provide significant legal protection, at least in the near term, such a safe harbor may not prompt voice providers to commit the resources necessary to develop sophisticated network-level call blocking programs.

starting to see these trends."[29] As one example, it is reasonable to expect that, as broader SHAKEN/STIR deployment makes it easier to trace a call to its origin, fraudsters may cycle through validly assigned numbers on a more frequent, rolling basis. Fraudulent schemes utilizing such an approach thus likely would evade blocking by providers that structure their blocking programs not to exceed the confines of a safe harbor premised on failed SHAKEN/STIR verification. This demonstrates the efficacy of adopting a safe harbor that is not tied to a call's verification under the SHAKEN/STIR standards, but instead protects existing call blocking programs and drives further innovation in the robocall mitigation space.

C. To Achieve the Commission's Policy Goals of Protecting Consumers From Illegal Robocalls, the Commission Should Adopt a Broad Safe Harbor for Voice Providers Implementing SHAKEN/STIR.

While AT&T does not believe that a call blocking safe harbor that is limited to calls that fail SHAKEN/STIR verification would effectively advance the Commission's policy goals, AT&T agrees that SHAKEN/STIR has a role to play in any safe harbor the Commission adopts. AT&T believes that a provider's implementation of SHAKEN/STIR demonstrates a sufficient commitment to addressing the robocall problem to warrant flexibility in the area of call blocking, subject to certain appropriate safeguards. AT&T thus renews its call for the Commission to adopt a safe harbor that would afford protection to providers that engage in provider-initiated call blocking if—despite reasonable best efforts—the provider inadvertently blocks a legitimate call.[30] Significantly, the Commission could limit the applicability of the broad safe harbor to providers that have implemented SHAKEN/STIR and, in so doing, achieve the goal of providing

---

[29] *See* Jonathan Nelson, Director, Project Management, Hiya, Statement at the July 11 Summit, at 1:34:12 – 1:34:25 (*"Nelson Statement"*).

[30] *See* Comments of AT&T, CG Docket No. 17-59, at 13-14 (filed July 20, 2018)(*"AT&T Comments"*). Ex Parte Letter from Linda S. Vandeloop, Assistant Vice President at AT&T, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, at 1 (filed Mar. 6, 2018).

a further incentive for providers to implement the standards.

Under AT&T's safe harbor proposal, the Commission would adopt a rule consistent with the following:

> **A voice service provider that inadvertently blocks a legitimate call shall not be deemed to have violated the Communications Act of 1934, as amended, or the Commission's rules, if, at the time the provider blocked the call, the provider:**
>
> > **(a) performed network blocking[31] of calls in connection with an event that the provider had a good-faith reason to believe was an illegal robocall event;**
> >
> > **(b) had procedures in place for network blocking that were reasonably likely to confirm that calls blocked were limited to illegal robocalls;**
> >
> > **(c) followed those procedures; and**
> >
> > **(d) had a process in place to unblock legitimate calls in the event of any inadvertent blocking of such calls.**

Such a broad safe harbor is critical to the battle against robocalls. Many in the industry already have the analytics and processes at their fingertips to make a bigger dent in illegal robocalls, but

---

[31] Provider-initiated blocking initiated by voice service providers is distinct from blocking pursuant to tools offered to consumers on an opt-in or opt-out basis. Provider-initiated blocking, as its name suggests, would not rely on consumer notice and consent (opt-in or opt-out). *See Consumer and Governmental Affairs Bureau Seeks to Refresh the Record on Advanced Methods to Target and Eliminate Unlawful Robocalls,* Public Notice, at 8114 n.1, CG Docket No. 17-59, (rel. Aug. 10, 2018)(DA 18-842) *("Record Refresh PN")* ("While third-party apps and other tools can help consumers avoid illegal calls, our focus here is voice service provider blocking of illegal calls without consumer consent or opt-in."); *see also Dec. Ruling and FNPRM* ¶ 23 (describing network-based blocking as "blocking without consumer choice"). In the recent *Declaratory Ruling*, the Commission rightly recognized that, in the context of consumer call blocking tools, rigid and prescriptive rules "could enable callers to evade blocking, and could impede the ability of voice service providers to develop dynamic blocking schemes that evolve with calling patterns." *Dec. Ruling and FNPRM* ¶ 34. The same reasoning extends to voice service provider-initiated blocking, and the Commission thus should embrace the same rationale for a call blocking safe harbor to further the Commission's policy goals and to more effectively protect consumers from illegal robocalls.

they simply lack the necessary incentive that a broad safe harbor would afford. Were the Commission to adopt a call blocking safe harbor consistent with AT&T's proposal, it would encourage industry to follow AT&T's lead in blocking more illegal robocalls. Further, to the extent the Commission requires SHAKEN/STIR implementation as a pre-condition to receiving safe harbor immunity, the safe harbor also would incent SHAKEN/STIR implementation by a broad range of providers. As such, the safe harbor proposal is fully consistent with the Commission's top consumer policy goal of ending the scourge of illegal and unwanted robocalls.[32]

AT&T's unique call-blocking program provides the basis for this broad safe harbor proposal, and can be used as a model for other providers to target and work to eliminate suspected illegal calls. At the network level, AT&T blocks calls that—after thorough analysis and investigation—AT&T's global fraud team reasonably determines are illegal. Under this program, AT&T compiles into a suspected robocall report aggregate call data that informs the detection of suspicious calls. As previously detailed in the record, these data include, but are not limited to: average call duration data, call completion rates, CNAM values, call volumes and the timeframes in which calls are placed, complaint data (including Commission and Federal Trade Commission ("FTC") complaint data), sequential dialing patterns, and call volumes to telephone numbers on the FTC's Do Not Call list. The report is updated on a virtually continuous basis. Based on the information in the suspected robocall report, AT&T investigates suspect telephone numbers, including but not limited to, a fraud investigator dialing the telephone number, and implements blocks on particular telephone numbers where there is reasonable basis to believe the

[32] *Stop Unwanted Robocalls and Texts,* FCC ("Unwanted calls – including illegal and spoofed robocalls – are the FCC's top consumer complaint and our top consumer protection priority.").

call is illegal.[33]

While some of the numbers blocked pursuant to this program fall within the scope of the *2017 Call Blocking* Order,[34] much of the suspected illegal traffic that AT&T identifies does not. AT&T's experience is consistent with other industry stakeholders. In particular, a recent report from TNS found that only 2 percent of the calls it scored as either "Nuisance" or "High Risk" actually originated from invalid or unallocated numbers (the kinds of numbers that the *2017 Call Blocking Order* deals with).[35] This finding confirms what AT&T already knows: to make a dent in the illegal and unwanted robocalls that are plaguing consumers, voice service providers need to block more calls than just those enumerated in the *2017 Call Blocking Order*.

Critically, by establishing a more flexible safe harbor, the Commission would avoid the unintended negative consequences discussed above.[36] For example, such a safe harbor would enable industry's efforts to combat illegal robocalls to evolve as the practices of bad actors evolve. Thus, the concerns noted above about stifling providers' innovation and experimentation, and creating loopholes for fraudsters to evade provider-initiated blocking programs, would not exist.

Likewise, as the Commission and other industry stakeholders have acknowledged, a

---

[33] *See AT&T Comments* at 10-11.

[34] The *2017 Call Blocking Order* authorized provider-initiated, network-level illegal call blocking for "calls from phone numbers on a Do-Not-Originate (DNO) list and those that purport to be from invalid, unallocated, or unused numbers." *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd. 9706, ¶ 1 (2017) ("*2017 Call Blocking Order*").

[35] Transaction Network Services, 2018 Robocall Investigation Report, at 7-8 (Oct. 2018), https://morningconsult.com/wp-content/uploads/2018/10/TNS_Robocall_Report_Oct18-_Final.pdf (last visited July 16, 2019).

[36] *See supra* Section I.B.

nexus exists between adopting a call blocking safe harbor and incenting greater SHAKEN/STIR deployment. SHAKEN/STIR information has an important role to play in provider blocking decisions—whether the information is incorporated into consumer blocking tools or as part of a provider-initiated call blocking program. Chairman Pai recently acknowledged this point when he observed that an appropriately tailored safe harbor "could not only give consumers more relief from spoofed robocalls, but also give voice service providers an additional incentive to implement SHAKEN/STIR promptly."[37] Similarly, the Commission acknowledged that the NANC CATA WG has reached the same conclusion.[38] A safe harbor whose protection is conditioned on SHAKEN/STIR deployment thus could provide voice providers with the added incentive to implement the protocols sooner rather than later, and perhaps even in the absence of a legal or regulatory mandate.

D. Consistent with Its Authority Under Sections 201 and 202, the Commission Should Broadly Define the Scope of Its Call Blocking Safe Harbor.

AT&T also urges the Commission to clarify that any safe harbor it adopts protects providers from liability even when, despite reasonable best efforts, they inadvertently block *legal* calls. As the Commission already has confirmed, call completion rules do not apply to *illegal*

---

[37] *See* Ajit Pai, Chairman, FCC, Remarks at the USTelecom Forum: Turning the Tide on Illegal Robocalls, at 2 (June 11, 2019).

[38] *NANC CATA WG Report* at 10 § 4.

calls.[39] As such, voice service providers do not require a safe harbor to block them.[40] Thus, any safe harbor established by the Commission must protect more than the blocking of illegal calls, and should extend to calls a provider blocks based on a reasonable call blocking program (whether legal or illegal, wanted or unwanted).

The Commission has ample authority to establish such a safe harbor. The Commission draws this authority from Sections 201 and 202 of the Act, which "have formed the basis for the Commission's historic prohibitions on call blocking."[41] Those sections prohibit unjust and unreasonable practices and unjust and unreasonable discrimination, and Section 201(b) specifically states that the Commission "may prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this chapter."[42] As the Commission concluded in its *2017 Call Blocking Order*, the blocking of certain robocalls is "not, by definition, an unjust or unreasonable practice or unjustly or unreasonably discriminatory."[43]

---

[39] The Commission has explained "that while voice service providers have a continuing obligation to transmit legal calls, that obligation does not extend to illegal calls, calls blocked with consumer choice, or calls for which the Commission has authorized blocking." *Dec. Ruling and FNPRM* ¶ 23 n.53.

[40] *Id. See also, Facilitating the Deployment of Text-to-911 & Other Next Generation 911 Applications*, Second Report and Order and Third Further Notice of Proposed Rulemaking, 29 FCC Rcd. 9846, ¶ 68 (2014) ("We find it unnecessary to adopt any 'safe harbor' provisions at this time. The only parties to date that have entered into a voluntary agreement to support text-to-911 are the CMRS provider parties to the Carrier-NENA-APCO agreement. Because the scope of the rules adopted in this *Second Report and Order* is consistent with the scope of their obligations under the voluntary agreement, there is no need for a 'safe harbor.'"); and *Cf. Smith v. City of Jackson, Miss.*, 544 U.S. 228, 238 (2005) (explaining that a statutory provision declaring certain actions lawful was "simply unnecessary to avoid liability . . . since there was no prohibited action in the first place").

[41] *2017 Call Blocking Order* ¶ 60.

[42] 47 U.S.C. §§ 201, 202(b).

[43] *2017 Call Blocking Order* ¶ 60.

And indeed, in the *Opt-Out Call Blocking Declaratory Ruling* that accompanied the *FNPRM*, the Commission held—in the opt-out blocking context—that "[i]n short, . . . we find that opt-out call-blocking programs are generally just and reasonable practices (not unjust and unreasonable practices) under section 201 . . . ."[44] The same reasoning should apply in this context, especially given that both opt-out blocking tools and provider-initiated call blocking programs serve—and, in AT&T's view, are needed—to mitigate the same tremendous harms that result from illegal robocalls. Accordingly, the adoption of an appropriate safe harbor to empower voice providers to stem the tide of such illegal calls would be in the public interest and thus authorized by Sections 201 and 202 of the Act.[45]

Commission precedent regarding call blocking provides further support. In its *2001 Blocking Order*,[46] the Commission concluded that Section 201(a) of the Act "d[id] not require AT&T . . . to refrain from blocking" certain calls.[47] Among the reasons cited by the Commission in reaching that conclusion, it found that the underlying entity responsible for the calls was a "sham entity,"[48] whose sole purpose was to generate unlawful revenues.[49] The general

---

[44] *Dec. Ruling and FNPRM* ¶ 47.

[45] The Commission is entitled to deference when it makes determinations under Section 201(b). *Glob. Crossing Telecommunications, Inc. v. Metrophones Telecommunications, Inc.*, 550 U.S. 45, 47–48 (2007) (citing *Chevron U.S.A. Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837, 843–44 and n.11 (1984)) ("In our view, the FCC's application of § 201(b) to the carrier's refusal to pay compensation is a reasonable interpretation of the statute; hence it is lawful.").

[46] *In the Matter of Total Telecommunications Services, Inc. and Atlas Telephone Company, Inc. v. AT&T Corp.*, Memorandum Opinion & Order, 16 FCC Rcd. 5726 (Mar. 8, 2001) (FCC 01-84) ("*2001 Blocking Order*").

[47] *2001 Blocking Order* ¶ 21.

[48] *Id.* ¶ 14.

[49] *Id.* ¶ 13.

characteristics of the scheme identified in the *2001 Blocking Order* bear strong resemblance to those of many illegal robocallers, who often operate outside the confines of legitimately established organizations, and whose robocalls are designed to generate revenues through unlawful means. Blocking the traffic of suspect illegal robocallers—regardless of the numbering resources on which they rely—is an inherently just and reasonable practice designed, in the words of one analytics expert at the Commission's July 11 Summit, to "shift all of this pain that we are receiving from these illegal robocallers, from consumers to the profit lines of the callers making them."[50]

Furthermore, given the acknowledged need for voice providers to continue to evolve best practices to combat illegal and unwanted robocalls, the Commission should avoid suggesting that calls covered by any safe harbor necessarily represent the outer limits of practices that would be deemed just and reasonable under Section 201.[51] Indeed, as illegal and unwanted robocalls continue to plague consumers and bog down networks,[52] no act of the Commission should suggest that providers, when acting reasonably, take *less* aggressive action to combat illegal robocalls.[53] To the contrary, the Commission should continue to promote its top consumer protection priority by facilitating provider efforts to lean in on all fronts to address this serious and growing consumer issue.

---

[50] *See Nelson Statement* at 1:34:31 – 1:34:45.

[51] As the Commission found in its 2001 Blocking Order, providers may more aggressively target illegal or unwanted calls consistent with Section 201 of the Communications Act and the Commission's precedent. *2001 Blocking Order*; *see also* 47 U.S.C. § 201.

[52] *See FCC Robocall Report* ¶ 7 ("Available data indicate that robocall volume remains high and may be increasing.").

[53] *See The FCC's Push to Combat Robocalls & Spoofing*, FCC ("By proposing and implementing effective policy initiatives and pursuing targeted enforcement actions, the FCC has been taking a bold stand to protect and empower consumers.").

In sum, the Commission should adopt a broad framework—based on AT&T's innovative call blocking program—to encourage other responsible providers to more aggressively fight against illegal robocalls. The safe harbor should protect well-meaning voice service providers from liability when they inadvertently, despite best efforts, block legal calls. Adopting the type of safe harbor proposed by AT&T is well within the Commission's legal authority, and it also is fully consistent with the Commission's important policy goals. As such, adopting AT&T's proposed broad safe harbor will help the Commission and industry to better protect consumers and networks from the robocall epidemic.

II. THE COMMISSION SHOULD FURTHER EMPOWER VOICE PROVIDERS TO ENGAGE IN ADDITIONAL ROBOCALL BLOCKING MEASURES, INCLUDING BLOCKING VOICE PROVIDERS ORIGINATING OR FACILIATING ILLEGAL ROBOCALL TRAFFIC

In addition to establishing an appropriate safe harbor to encourage voice service providers to block more illegal robocalls, AT&T welcomes the Commission's proposals of additional measures to enhance the ability of industry to prevent such calls from ever reaching consumers. AT&T is particularly interested in the proposal to establish a framework to identify and target voice service providers that facilitate and fuel illegal and unwanted robocalls—including by blocking traffic based on the identity of the originating provider. Consistent with the statements of admitted fraudster Adrian Abramovich, AT&T believes that there likely are a handful of providers responsible for delivering the vast majority of illegal robocalls to consumers via the public switched telephone network ("PSTN"). Taking aggressive action to target calls from these providers would pay dividends, but it is important that the Commission proceed with caution to ensure that any legitimate customers of these providers are not impacted by any such provider-specific blocking framework.

As Chairman Pai observed in his statement accompanying the *FNPRM*, a

"comprehensive strategy to combat"[54] the robocall scourge is needed, and a framework targeting voice providers that facilitate illegal robocalls would be a highly effective component of the Commission's comprehensive strategy. In particular, while much of the focus has been on deploying tools to consumers to stop calls on the receiving end, targeting voice providers that facilitate such calls would stop these calls at or near their point of origin. Moreover, enabling voice providers to target providers responsible for originating significant volumes of illegal robocall traffic is complementary to AT&T's continued belief that more vigorous enforcement activity is necessary to more effectively address the robocall problem.

Given the importance of stopping illegal robocalls at their source, AT&T supports the Commission's proposal to "target those voice service providers that are most likely to facilitate unlawful robocallers."[55] AT&T agrees that it is possible, if not likely, that certain providers will attempt to undermine or abuse the SHAKEN/STIR framework. While it may be too early to determine precisely what form(s) such abuse could take,[56] the Commission should not limit its consideration of punitive action to those providers that do not "appropriately sign" their traffic.[57]

---

[54] *Dec. Ruling and FNPRM* (Statement of Chairman Ajit Pai).

[55] *Id.* ¶ 55.

[56] During the Commission's July 11 Summit, several expert panelists discussed the fact that bad actors will identify methods and practices to deceptively evade SHAKEN/STIR and robocall blocking measures. *See e.g. Nelson Statement* at 1:34:12-1:34:25 (noting that industry is facing "intelligent adversaries" that are "actively trying to fight back against companies" blocking their calls, and that these same adversaries "will be reacting to STIR/SHAKEN, and we are already starting to see these trends."); *see also*, Ram Ramanathan, Product Management, Ribbon Communications, Statement at the July 11 Summit, at 3:39:28 – 3:39:50 (noting that flexibility in the deployment of SHAKEN/STIR and robocall mitigation efforts are important, since this is "an evolving area" and that "there are ways that robocallers can figure out, using a different trap door or back door to get back in."); *Hambuchen Statement*, 1:47:11-1:47:25 ("So this is not a static issue. As we figure out ways to block or identify or deal with those unwanted or illegal calls, the bad guys will continue to look for ways to get their calls through.").

[57] *Dec. Ruling and FNPRM* ¶ 55.

Rather, the Commission instead should establish a framework that would enable the identification of particularly egregious providers that facilitate illegal robocalls, and then encourage and empower industry stakeholders to take appropriate countermeasures—up to and including the blocking of traffic associated with such providers—while simultaneously leveraging the full weight of the Commission's authority and law enforcement to permanently put bad actors out of business.

It is no secret that, while most voice service providers are moving to rid their networks of illegitimate traffic associated with such calls, other providers are either indifferent to, or active in, the generation of illegal robocall traffic. In his 2018 Senate testimony, Adrian Abramovich noted that the VoIP providers that actively solicit customers for "short duration calls" are critical to the proliferation of illegal robocalls that has occurred and continues today. Abramovich noted that companies advertising for such traffic will accept "all the calls you can throw at them," and that such providers "never ask" about the caller ID information used by their customers. Abramovich undoubtedly was correct when he stated that such providers are "fueling" illegal robocall traffic, and that it would be a "good idea" to focus on the "five or six companies" responsible.[58] While an exact number of companies responsible for generating such traffic may currently be unknown, the ability to identify at least some of them exists, due in no small part to USTelecom's Industry Traceback Group ("ITB Group"), including recent enhancements made to the traceback process that allow the group to more rapidly and accurately identify the source of

[58] U.S. Senate Committee on Commerce, Science, & Transportation, Hearing, *Abusive Robocalls and How We Can Stop Them*, at approx. 1:03:03 (Apr. 18, 2018) https://www.commerce.senate.gov/public/index.cfm/hearings?ID=E0EB17D2-A895-40B4-B385-F94EA2716957 (last visited July 11, 2019).

illegal robocall traffic,[59] *and* increased and more formalized collaboration between industry and government stakeholders.[60]

As the Commission has previously acknowledged, it already has an exceptional working relationship with the ITB Group, and this should used to identify voice providers facilitating

---

[59] Through its automated traceback portal—which has reduced traceback times from weeks to "sometimes . . . hours"—the ITB Group is able to identify providers that are often the source of illegal robocall traffic. Kevin Rupy, Partner, Wiley Rein, Representing US Telecom – The Broadband Association, Statement at the United States Senate Subcommittee on Communications, Technology, Innovation, and the Internet, *Abusive Robocalls and How We Can Stop Them*, at 1 (Apr. 18, 2018), https://www.commerce.senate.gov/public/index.cfm/2019/4/illegal-robocalls-calling-all-to-stop-the-scourge (last visited July 11, 2019).

[60] For example, over the last several years, the FTC has convened four workshops with the U.S.-India Business Council. These workshops brought together representatives from U.S. and foreign enforcement and private sector stakeholders, who focused on technical defenses, law enforcement, consumer and business education, and international coordination efforts to tackle Indian call-center fraud. FTC, Statement Before the United States Senate Committee on Commerce, Science and Transportation, Prepared Statement of The Federal Trade Commission, Before the United States Senate Committee on Commerce, Science and Transportation, *Abusive Robocalls and How We Can Stop Them*, at 15 (Apr. 18, 2018), https://www.ftc.gov/system/files/documents/public_statements/1366628/p034412_commission_testimony_re_abusive_robocalls_senate_04182018.pdf (last visited July 11, 2019). One product of this collaboration was the enforcement action in India against a massive telemarketing fraud ring operating outside Mumbai, which resulted in the arrest of 70 people and detention of more than 700 employees. Rama Lakshmi, *Mass arrests made in IRS phone scam*, The Morning Call (Oct. 6, 2016), https://www.mcall.com/business/mc-india-call-center-irs-scam-arrests-20161006-story.html (last visited July 18, 2019). Similarly, AT&T continues to independently pursue collaborative efforts with partners in government, including the recent participation of Bruce Byrd, Chief Legal Officer of AT&T Communications, in a Department of Justice (DOJ) industry forum on tech-support fraud, which U.S. Attorney General William Barr hosted. *See* AT&T Blog, *AT&T Highlights Efforts to Combat Robocalls at U.S. DOJ Industry Forum on Tech Support Fraud* (Apr. 3, 2019), https://www.attpublicpolicy.com/congress/att-highlights-efforts-to-combat-robocalls-at-u-s-department-of-justice-industry-forum-on-tech-support/ (last visited July 17, 2019).

robocall traffic.[61] For example, the Enforcement Bureau could again publicly identify voice providers associated with illegal robocall traffic that consistently decline to cooperate with the efforts of the ITB Group.[62] In instances where a particular provider repeatedly appears in separate traceback investigations, but declines to identify the source of the traffic, the Commission could consider publicly identifying the provider and using that public notice to trigger additional processes that would culminate in the provider's eligibility for blocking by other providers. Moreover, it is possible, if not likely, that the bad actors that decline to support the efforts of the ITB Group would be the same entities likely to attempt to circumvent or subvert the SHAKEN/STIR process. Consistent with AT&T's other efforts, AT&T would welcome the opportunity to work with the Commission and other industry stakeholders to further consider appropriate ways to target bad actors in the communications ecosystem and eliminate their illegal robocall traffic.

CONCLUSION

AT&T applauds the ongoing efforts of the Commission to address the serious issue of illegal and unwanted robocalls. AT&T supports the Commission's proposal to adopt a call blocking safe harbor and urges the Commission to ensure the safe harbor covers providers that, together with deploying SHAKEN/STIR, implement reasonable call blocking programs, including when such a provider inadvertently and in good faith blocks a legal call. By adopting

---

[61] *See*, Letter from Rosemary C. Harold, Chief, Enforcement Bureau, FCC, and Eric Burger, Chief Technology Officer, FCC, to Jonathan Spalter, President & CEO, USTelecom – The Broadband Association (Nov. 6, 2018), https://docs.fcc.gov/public/attachments/DOC-354942A2.pdf (last visited July 11, 2019) (noting that the efforts of USTelecom's ITB Group had reduced the Enforcement Bureau's own traceback investigations from "months to weeks," and that the Bureau "look[ed] forward to building on the foundation of the past two years and achieving even greater success in the future.").

[62] *Id.*

such a safe harbor framework, the Commission can better achieve its goals of increasing the deployment of SHAKEN/STIR, while significantly enhancing the ability of voice providers to protect their customers from illegal robocalls. As the fight against illegal and unwanted calls continues, AT&T looks forward to continuing to work closely with the Commission to develop additional solutions for the benefit of consumers.

Respectfully submitted,

/s/ Kevin G. Rupy

Amanda E. Potter
Gary L. Phillips
David Lawson
AT&T SERVICES, INC.
1120 20th Street, NW
Washington, DC 20036

Kevin G. Rupy
Kathleen Scott
WILEY REIN LLP
1776 K Street, NW
Washington, DC 20006

July 24, 2019